通鼎互联信息股份有限公司审核案例

撰写者：李治纲

【案例摘要】

办公、生产信息化和智能化程度越高的企业，其对信息安全、网络安全需求和期望越高，存在信息安全风险也越多，需要加以控制。

一、案例背景介绍

推荐机构：方圆标志认证集团有限公司

案例类型：管理体系认证

认证类型：信息安全管理体系

受审核方名称： 通鼎互联信息股份有限公司

审核依据： GB/T22080-2016 ISO/IEC 27001:2013

审核时间： 2018 年 7 月 4~6 日

审核范围：位于江苏省苏州市吴江区震泽镇八都经济开发区小平大道 8 号的办公楼、电缆车间、数据缆车间、光缆一部 3#车间、光缆二部车间、光缆四部车间、光纤三期车间、射频电缆车间、电力电缆车间、仓库的通鼎互联信息股份有限公司的光纤、市内通信电缆、局用同轴电缆、通信电源阻燃耐火软电缆、数字通信用水平对绞电缆和 XDSL 传输引入电缆的生产；通信光缆、射频及泄漏同轴电缆的设计和生产相关的信息安全管理活动。信息安全适用性声明：B/0。

审核组长：李治纲 **审核组员：吴荣华、石小平、朱亚军**

二、受审核方基本情况

受审核方为一家主要从事光纤光缆、通信电缆、铁路信号电缆、城市轨道交通电缆、RF 电缆、特种光电缆、光器件仪器仪表、机电通信设备、线缆及配套产品的研发、生产、销售和工程服务的企业。2010 年 10 月 21 日，在深交所成功上市（股票代码：002491）。2017 年开始对公司进行智能化制造改造，对相关车间进行网络化、自动化、智能化改造，为了加强信息安全管理，使用体系化思路管理信息安全，为此企业 2017 年按 ISO/IEC 27001：2013 标准建立信息安全

管理体系，不但加固了本身信息安全这个“堤坝”，还倡导本行业各类企业使用ISO/IEC 27001：2013管理企业各类信息资产。

三、主要审核发现、沟通过程

名称解释：

- SQL注入攻击（SQL Injection）：简称注入攻击、SQL注入，被广泛用于非法获取网站控制权，是发生在应用程序的数据库层上的安全漏洞。在设计程序，忽略了对输入字符串中夹带的SQL指令的检查，被数据库误认为是正常的SQL指令而运行，从而使数据库受到攻击，可能导致数据被窃取、更改、删除，以及进一步导致网站被嵌入恶意代码、被植入后门程序等危害。
- 静态NAT（网络地址转换）：指将内部网络的私有IP地址转换为公有IP地址，IP地址对是一对一的，是一成不变的，某个私有IP地址只转换为某个公有IP地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备（如服务器）的访问。
- Telnet:是一种明码通信协议是TCP/IP协议族中的一员,是Internet远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机(或远端设备)工作的能力。在终端使用者的电脑上使用Telnet程序，用它连接到服务器（或远端设备）。终端使用者可以在telnet程序中输入命令，这些命令会在服务器（或远端设备）上运行，就像直接在服务器（或远端设备）的控制台上输入一样。可以在本地就能控制服务器。
- SHH：是一种加密通信协议是TCP/IP协议族中的一员，建立在应用层基础上的安全协议，功能与Telnet一致。
- 弱口令(weak password)：没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。

2018年7月4~6日上午受方圆标志认证集团有限公司的委托李治纲、吴荣华、石小平、朱亚军等4人，对通鼎互联信息股份有限公司进行信息安全管理体系初审（二阶段）现场审核，审核组组长编制审核计划，确定审核主要审核企业信息

化部、设备部、综合部、人力资源部、财务部、商务部、市场经营部、供应链管理部、质量管理部、生产经营部、后勤保障部、海外及企业业务部、电缆车间、数据缆车间、光缆一部 3#车间、光缆二部车间、光缆四部车间、光纤三期车间、射频电缆车间、电力电缆车间，以及相应的资产识别、风险评估和风险控制措施。

现场审核，审核组现场取证发现：

第一：用于该公司对外宣传的网站（http://www.tongdinggroup.com/）主机及数据库存放公司内网 WEB 服务器中，通过在防火墙中 NAT 方式映射到外网，而此主机与内网的其它网络及服务器没有进行任何隔离措施。

开具不符合原因：通过 NAT 方式进行映射，貌似可以在不对外公开 WEB 网服务器信息的前提下，提供外网网站访问，但 NAT 的同时也向全世界公开了公司共有 IP 地址，黑客可以扫描漏洞方式进行网络攻击。同时，外网蠕虫病毒、木马病毒、勒索病毒可以通过 WEB 服务器作为跳板传染到内网中其他服务器和设备中，极易造成网络故障、信息外泄等信息安全风险。故开具一份不符合报告

不符合：GB/T22080-2016 ISO/IEC27001:2013 A.13.1.3 组织应在网络中隔离信息服务、用户及信息系统。

第二：受审核方网络层级比较多，有多个路由器、防火墙、交换机等网络设备，对这些设备访问、控制是通过 Telnet 进行远程操作的，但 Telnet 是明码协议。

开具不符合原因：由于受审核方内部办公网、生产网没有物理隔离，只要在相关网段的计算机中安装一个网络监听工具，就可以截获网络所有明码通信内容，通过分析和整理，完全可以获取登录设备的账号和密码，这类软件如 Wireshark。故开具一份不符合报告。

不符合：GB/T22080-2016 ISO/IEC27001:2013 A.13.2.3 应适当保护包含在电子消息发送中的信息。

第三：北京百卓网络技术有限公司 2018 年 5 月份对公司网络中运行设备、软件系统中存在的问题进行漏洞扫描，发现 20 项目安全隐患（含技术脆弱性），如 SQL 注入、弱口令、海康威视权限认证等漏洞，但没有形成对 20 项安全隐患（风险）的正式处置措施，以及后续整改的证据。

开具不符合原因：既然第三方检测公司对网络中的设备及软件开具“病情”诊断报告，且大部分是常见信息安全漏洞或风险，如不加以应对受审核方极易出现大规模病毒爆发情况，严重影响日常办公和生产，且受审核方信息主管部门和相关领导对这份检测报告，在意识根本不重视，总以为不会发生检测报告提示到信息安全风险。故开具一份不符合报告。

不符合：GB/T22080-2016 ISO/IEC27001:2013 A.12.6.1 应及时获取在用的信息系统的技术方面的脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。

经与受审核方确认了上述三项目不符合，为一般不符合报告，给 30 天整改，需要采取纠正和纠正措施，审核组采取异地验证方式。

一、 不符合报告整改和验证

受审核方对不符合报告采取纠正和纠正措施进行整改，分别是：

第一份：

原因分析：未意识到存在风险，只是想便于日常维护和管理，且早期未购买云服务，故网站一直放于本局域网内，通过端口映射方式来提供。

纠正：购买阿里云服务，编制“迁移”方案，按方案把网站迁移至阿里云服务器中，与公司公网 IP 隔离。

纠正措施：对标准要求、迁移技术、域名指向设置和网页绑定技术等进行了培训，提高信息安全管理意思和技术能力。

验证：提供 1 份纠正和预防措施处理单， 1 份培训记录表， 1 份网站迁移整改方案，提供迁移前后对比截图， 1 份网站迁移实施记录（含网站在云服务中正常运行截图、防火墙端口映射关闭截图等），经异地书面和在线测试验证，基本接受。

第二份：

原因分析：近期需要对可登录 IP 范围和网络进行比较频繁调试，为了调试方便打开 Telnet。

纠正：关闭 Telnet 协议，使用 SSH2 加密协议进行网络调试。

纠正措施：对标准要求，Telnet、SSH 比较，为什么对交换机和防火墙进行操作时应使用加密协议等进行培训，达到预期目标。同时举一反三发现 SNMP

协议通信字符串为 Public 属性，有网络结构外泄的风险，培训后修改此属性。

验证：提供 1 份纠正和预防措施处理单，1 份培训记录表，1 份 Telnet 关闭截图，1 份 SSH2 协议启动截图，2 份通过 SSH2 操作远程设备的截图。经异地书面验证，基本接受。

第三份：

原因分析：意思不强，未对 20 项安全隐患做整改方案，也未保留整改相关证据。

纠正：对 20 项安全隐患编制整改方案，按整改进行整改，保留相关证据。

纠正措施：对标准要求，常见漏洞简介与处置，SQL 注入危害，WEB 中其他漏洞，WSUS（微软公司提供的网络化的补丁分发方案）设置与使用等进行培训，使参会人员提高奥信息安全意识，知道相关漏洞的危害性，并统一补丁升级技术手段（WSUS）。

验证：提供 1 份纠正和预防措施处理单，2 份培训记录表，1 份整改方案，1 份整改过程记录（如系统升级、安装网站安全防御狗、关闭 U8 系统 WebDav 扩展服务、关闭 oracle 数据库监听服务等）。经异地书面验证，基本接受。

四、受审核组织主要的改进方法及其成效

通过上述三份不符合报告内容，我们看到部分企业负责人对信息安全不重视、无所谓，只知道企业要实现信息化，为此投入大笔资金，但信息化后的信息安全风险往往不特别关注，除非发生一次重大信息安全事件后，才后悔。通过对不符合整改，看似给受审核方没有带来什么现实经济效益，但消除或降低受审核方存在信息安全风险，是无形的，是管控信息风险效益。

同时，企业信息主管部门通过对不符合报告整改，提高相关技术能力，再次认识到信息安全必须靠可靠的、先进的技术进行管控，且必须定期更新。

2014年02月27日在中央网络安全和信息化领导小组第一次会议的讲话:“没有网络安全就没有国家安全，没有信息化就没有现代化”

2016 年 4 月 19 日在在网络安全和信息化工作座谈会上的讲话:“维护网络安全，首先要知道风险在哪里，是什么样的风险，什么时候发生风险，正所谓“聪者听于无声，明者见于未形”。感知网络安全态势是最基本最基础的工作。要全

面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。……。网上信息管理，网站应负主体责任，政府行政管理部门要加强监管。”

五、总结

信息安全管理永远没有结束，永远在路上。